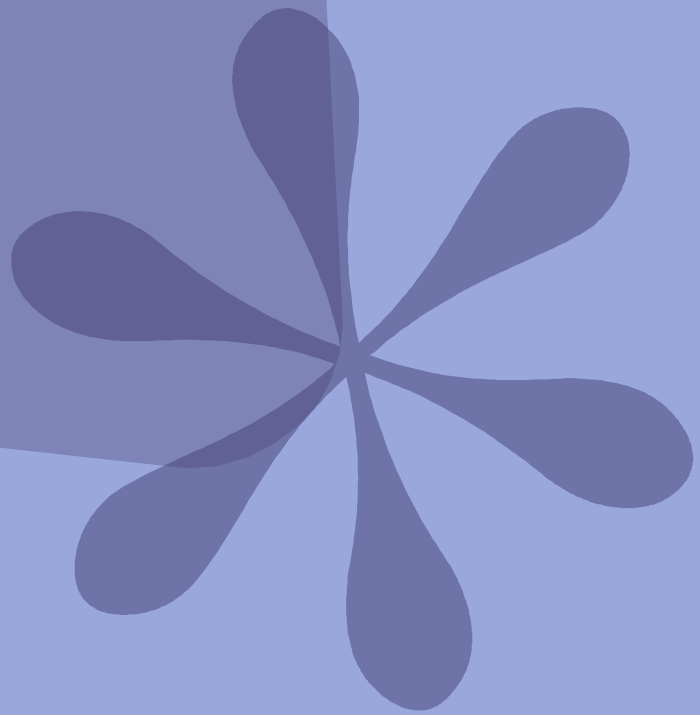
Detección de intrusiones en sistemas VoIP con SIP

Iria Prieto Suárez

16 Enero 2009



Índice

- Introducción
- Estrategias detección de intrusiones
- VoIP Intrusion Detection Through Protocol State Machines
- Estrategia a implementar

Introducción

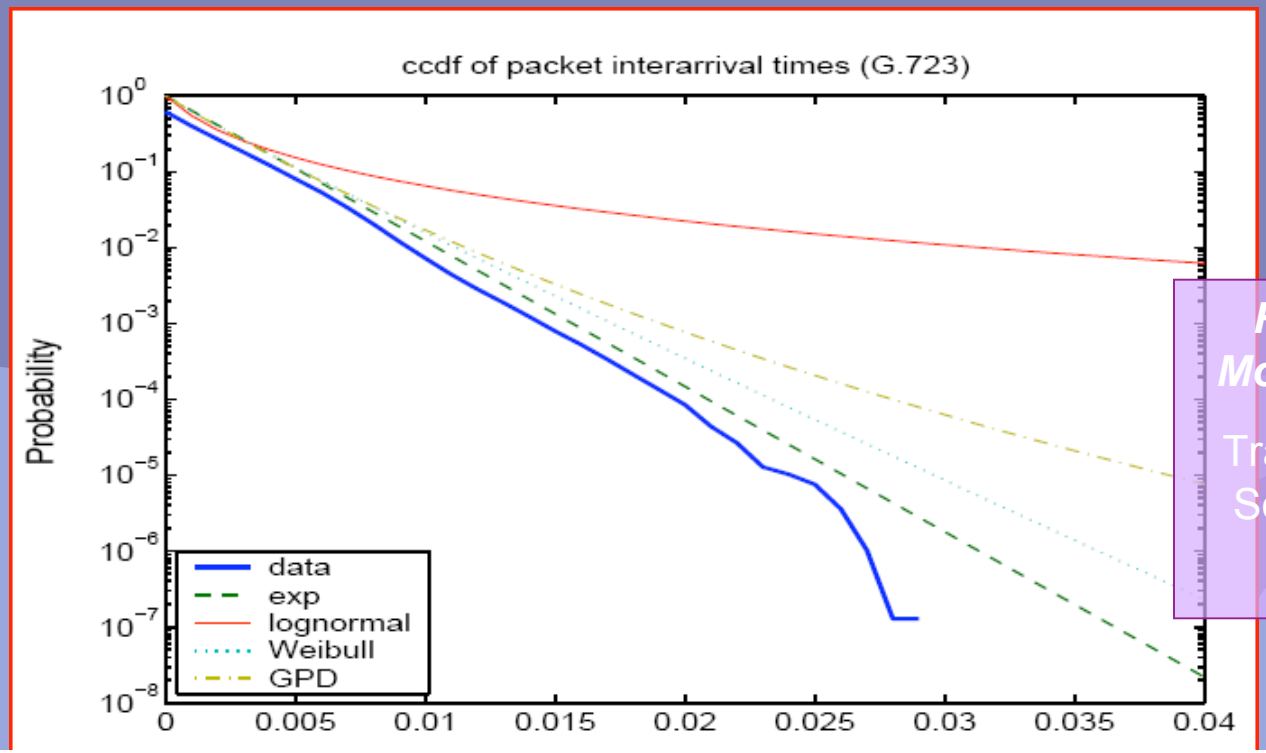
- Auge de las comunicaciones VoIP que emplean SIP
- Aumento de ataques a estos sistemas:
  - Denegación de Servicio (DoS)
  - Escuchas Ilegales/No autorizadas
  - Intercepción y Modificación
  - SPIT (Spam Over Internet Telephony)
  - VISHING (Voice Phising)

Estrategias detección de Intrusiones (I)

- Diferentes estrategias:
  - Patrones On-Off del tráfico RTP
  - Caracterización de perfiles y definición de reglas
  - Basados en el texto de los mensajes SIP
  - Máquinas de estados

Estrategias detección de Intrusiones (II)

- Patrones On-Off
  - Distribuciones de periodos On-Off
    - Ajuste exponencial
    - Dependientes de los Códecs
    - Sólo serviría para ataques basados en el RTP



Fractal Analysis and Modeling of VoIP Traffic

Trang Dinh Dang, Balázs Sonkoly, Sándor Molnár

2004

Estrategias detección de intrusiones (III)

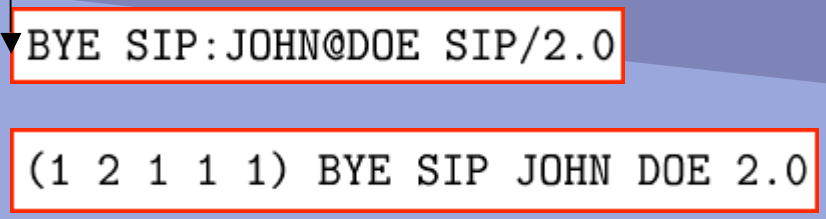
- Caracterización de perfiles y definición de reglas
  - Realización de estadísticas según roles
    - Nivel de Host
      - Número de mensajes enviados y recibidos
    - Nivel de servidor
      - Número de usuarios registrados satisfactoriametne
    - Nivel de usuario
      - Duración de una llamada
  - En cada nivel se definen reglas

```
Method=Register, diff_username_rate < 0,1% -> class guesspassword
```

A framework for detecting anomalies in VoIP Networks.
Yacine Bouzida and Christophe Mangin
2008.

Estrategias detección de intrusiones (IV)

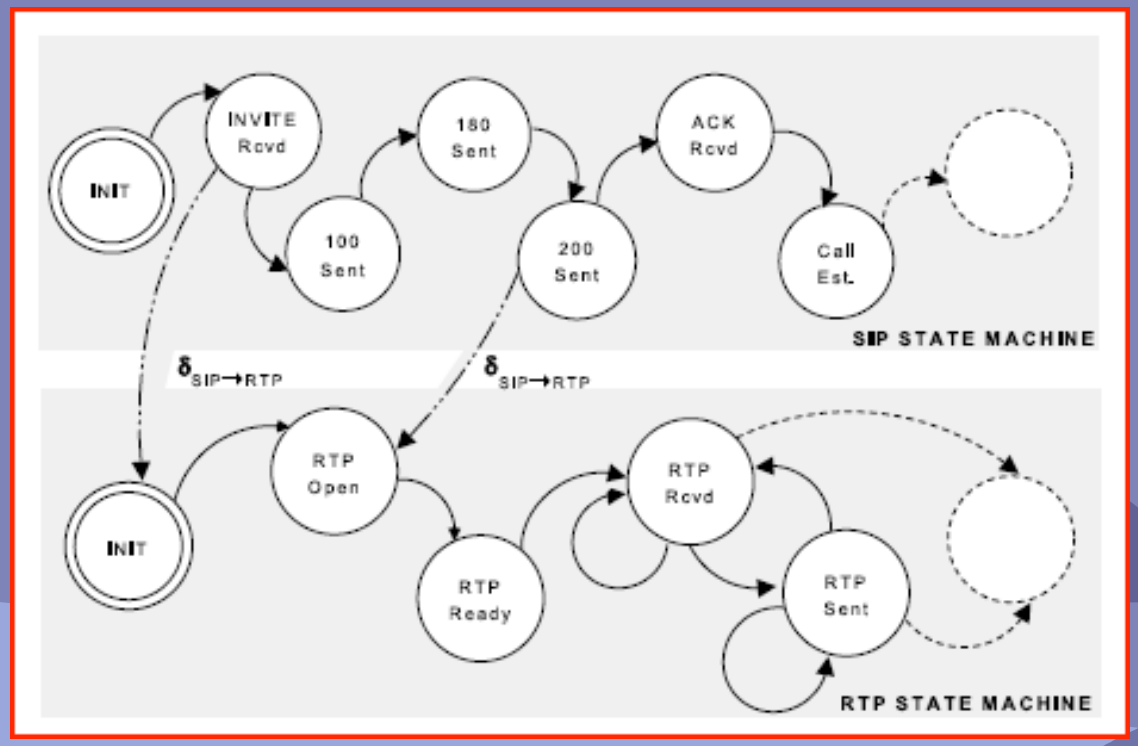
- Basados en el texto de los mensajes SIP
  - Detectan los ataques de tipo Fuzzing
  - Caracterizan cadenas de texto del tráfico bueno
    - Entrenamiento con trazas de tráfico buena
    - Reentranamiento cada cierto tiempo. Se calibran los umbrales



A self-learning system for detection of anomalous sip messages
Stefan Wahl Pavel Laskov Peter Domschitz Konrad Rieck and Klaus-Robert Müller.

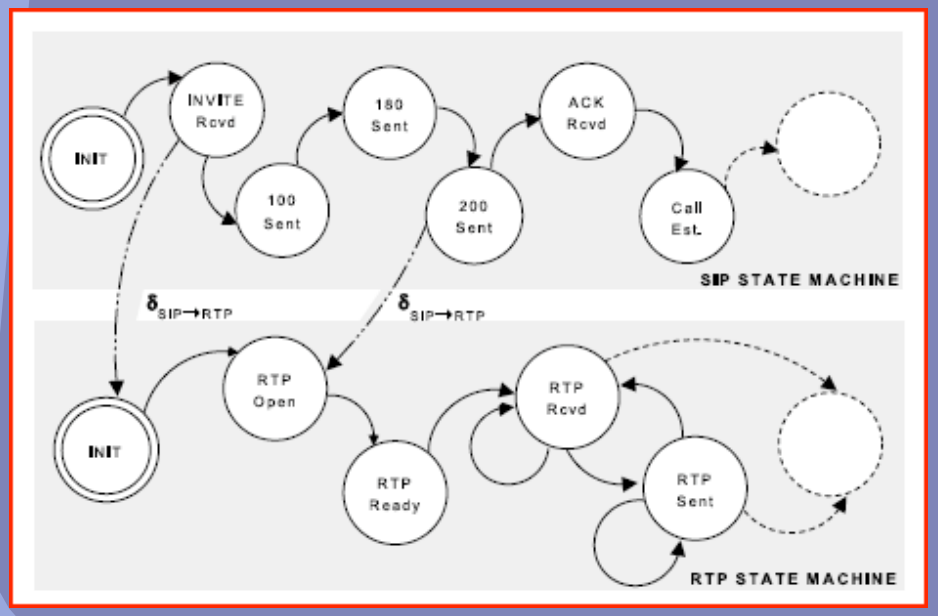
Estrategias detección de intrusiones (IV)

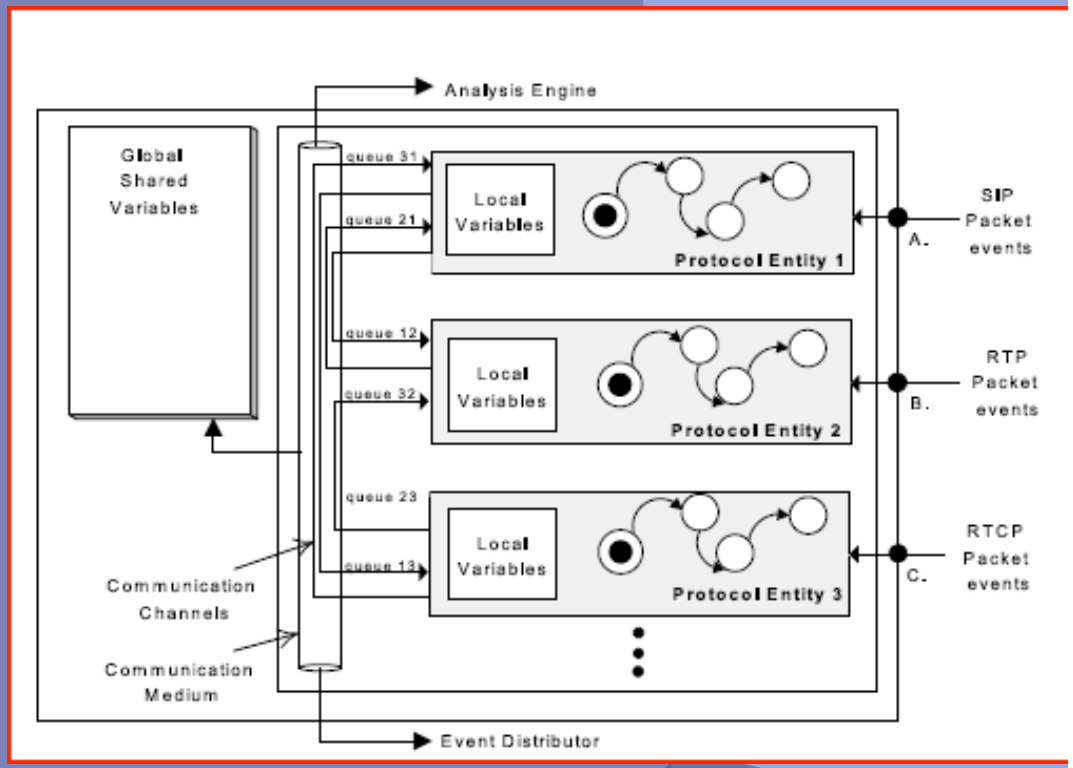
- Máquinas de estados
  - Se modelan diálogos para SIP y RTP



  - Se modelan máquinas para los ataques conocidos
  - Desventaja: No se detectan nuevos ataques

VoIP Intrusion Detection Through Interacting Protocol State Machines



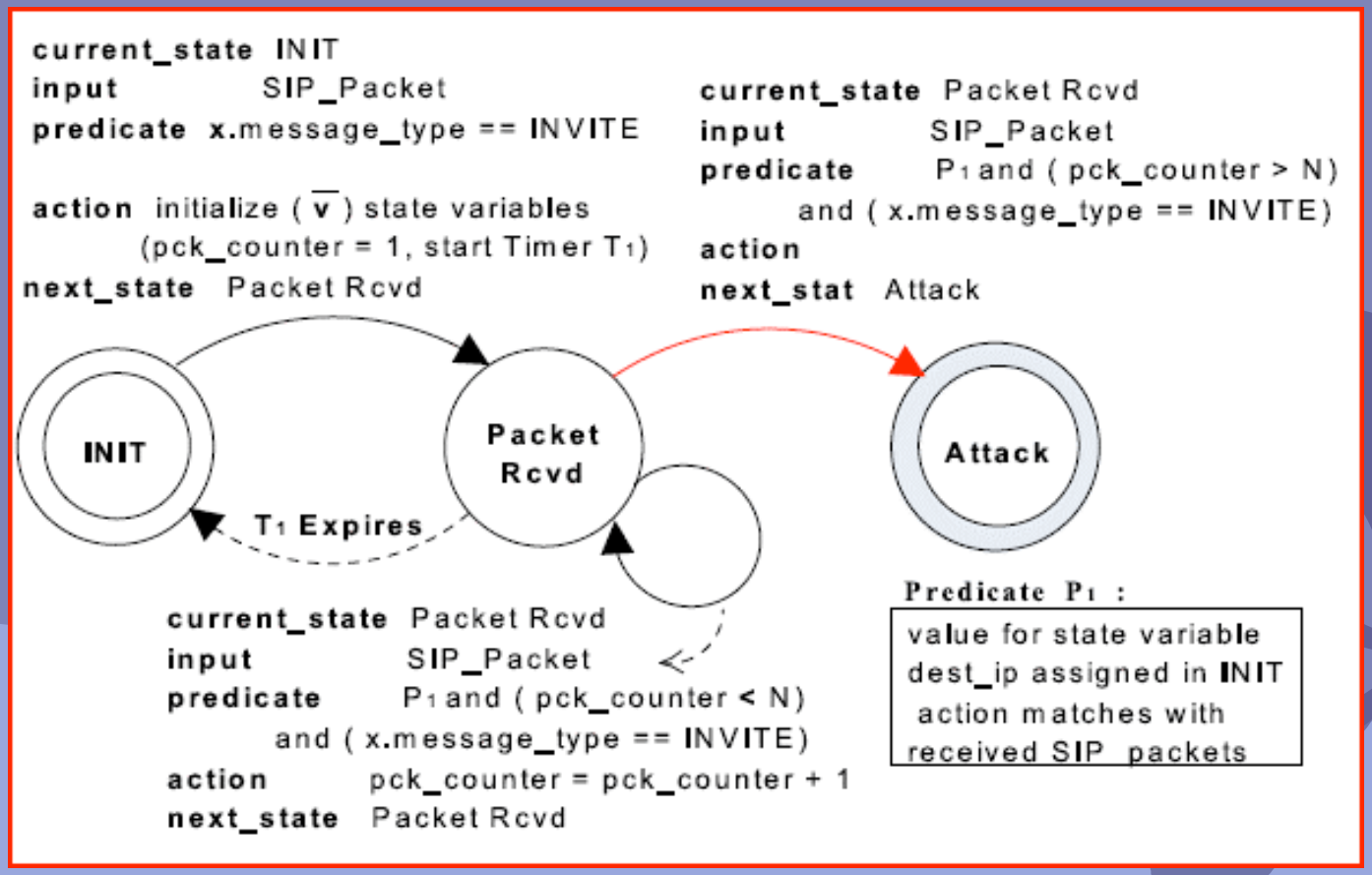


VoIP Intrusion Detection Through Interacting Protocol State Machines

Hemant Sengart, Duminda Wijesekera, Haining Wang, Sushil Jajodia

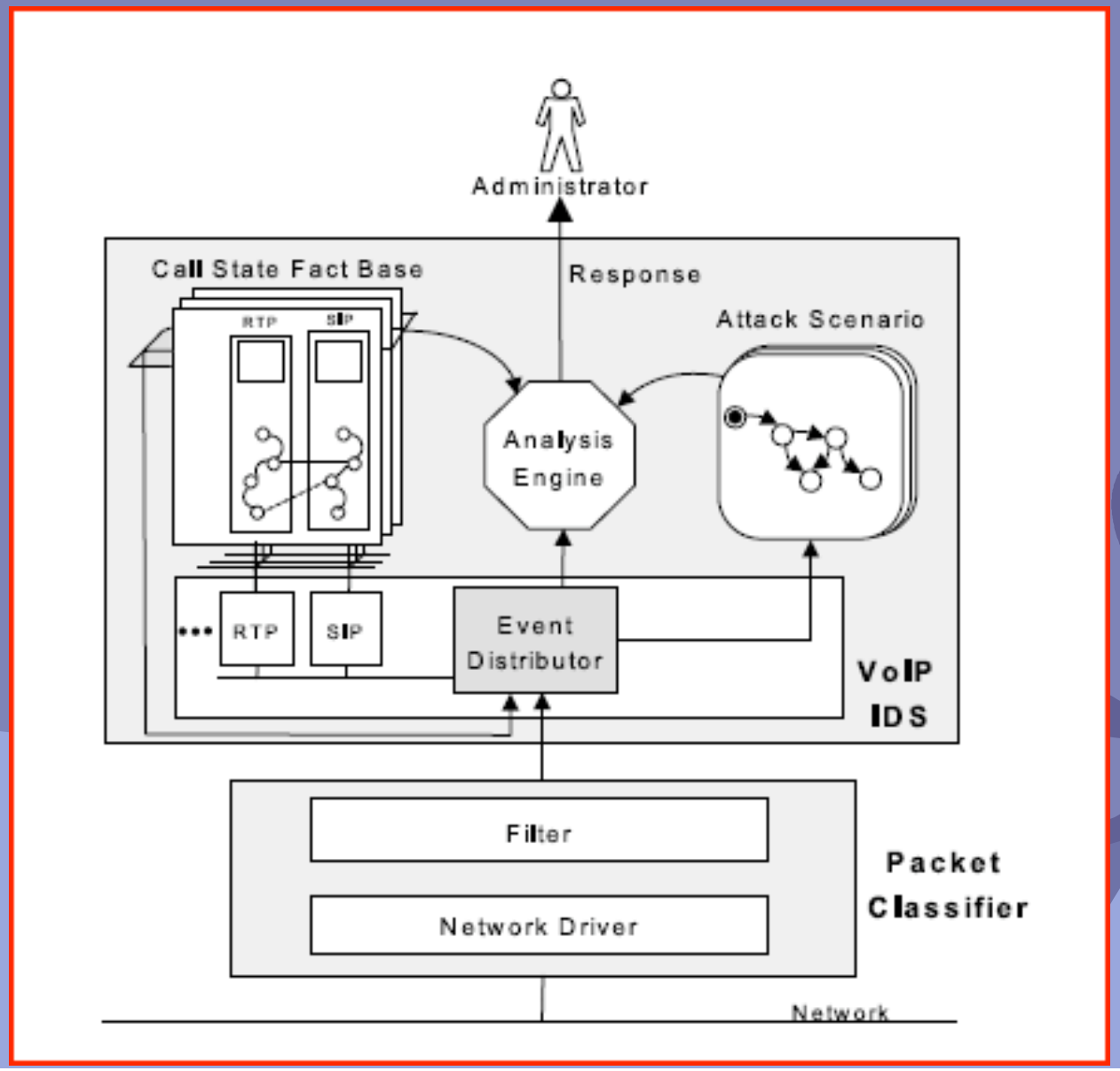
2006

VoIP Intrusion Detection Through Interacting Protocol State Machines



Ataque INVITE FLOODING

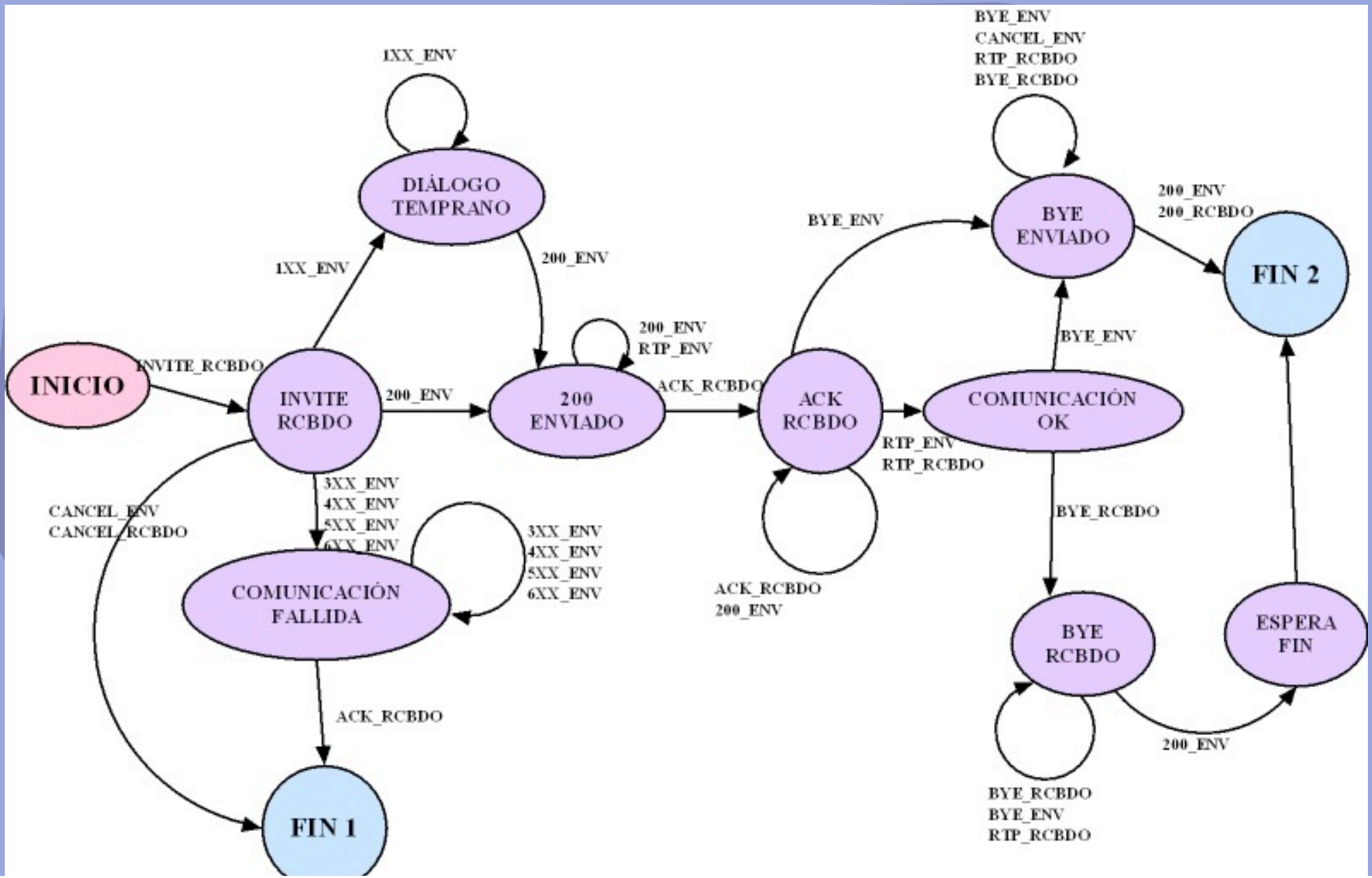
VoIP Intrusion Detection Through Interacting Protocol State Machines



Estrategia a implentar (I)

- Máquina de estados de una comunicación buena
- Para comportamientos inesperados se va a un estado de error
- Para detectar los ataques utilizar técnicas de Clustering sobre el Estado de Error

Estrategia a implementar (II)



Preguntas y sugerencias